

DOCUMENT-IDENTIFIER: US 3798360 A  
TITLE: STEP CODE CIPHERING SYSTEM

----- KWIC -----

DWKU:  
3798360

ABPL:

The multiple level encipherment process is also utilized in a variant key embodiment which would encipher a data block D into a cipher C which is a function of a key control block consisting of a random combination binary digits that are continuously changing.

BSPR:

It is a further object of the present invention to provide a cryptographic communication system wherein the cipher is developed under the control of two separate keys, a block of binary digits associated with each subscriber of the system, and a random set of binary digits which are simultaneously available at both transmitting and receiving stations within the communications system.

BSPR:

In a second embodiment, a cipher process is presented for developing a variant cipher which is dependent on the binary levels of the input data itself. In the process, a random combination of binary digits is utilized to form the key for operating the cryptographic device that develops the first cipher block. Then, a portion of the first cipher block is stored and the remaining portion is combined with the same randomly generated binary digits to form a second ciphertext. The second ciphertext and the stored portion of the first cipher text are then combined to form a new composite cipher block

that is  
transmitted.

DEPR:

The above description of the system shown in FIG. 1 illustrates the cipher and decipher operation under the control of the user key K and  $K_{sup.1}$ . In certain instances where it is desirable to have a higher degree of data security, the clear data is enciphered under the control of two separate and distinct keys in a multiple encipherment process. The degree of security as used within this specification relates to the probability of guessing the unique combination of key binary digits by an opponent having both the knowledge of the internal circuitry of the system and the opportunity to observe prior transmissions and resulting ciphers. The variant option which operates under control 42 applies a combination of binary bits identified as R during the first enciphering operation in the multiple cipher process. The unique combination of binary digits R are introduced into cryptographic system 22 by applying a control signal  $C_{sub.2}$  to gate 44 which enables a random number key generator 43 to supply some unique continuously varying combination of binary digits to a key register within the cryptographic system 22. This same random number consisting of a random arrangement of binary digits is simultaneously loaded into one of the segments of the data block appearing in feed register 20. An exemplary random number generator may be found in U.S. Pat. No. 3,366,779, issued Jan. 30, 1968. Also, it is possible to compute a set of random numbers in accordance with the teachings in Handbook of Mathematical Functions, U.S. Department of Commerce, National Bureau of Standards, Applied Mathematics Series 55, 1964, Chapt. 26, Sec. 8, and store a

table of random numbers for further access. Note that if the random control key R requires a greater dimension of binary digits than is available in the actual random number generated, the number developed by random number generator 43 may be padded with some fixed combination of bits.

DEPR:

In the deciphering operation at the receiver station, the variant control key R.sup.-.sup.1 is provided by an identical random number generator 43' operating in synchronism with the generator 43 in the transmitter. The only additional feature provided in the deciphering sequence is an additional error-checking facility which is carried out by comparator 50. Both the receiver and transmitter stations, which at any point of time could be either the terminal or CPU within a data processing network, have an identical random number generator 43. Thus, upon deciphering the subgroup C' which consists of the random number R, a comparison check is performed. A mismatch detected by comparator 50 indicates that an error is present due to either a faulty transmission line or a processing error created by the cryptographic systems 22 or 22'.

DEPR:

During the first round of the cryptographic system, the mangler 30 performs no initial operation on the message data D. The lower 24 bits within the storage elements 41a-64a are loaded into a plurality of gates G and G, each pair of gates receiving one output from the mangler 30. For example, gates 325 and 326 receive the output line from lower storage element 41a. The quadruplet of shift registers which receive the quadruplet of information n lines have associated therewith a set of four pairs of gates G and G, each gate being

activated by one of the control lines 300, 301 and 302. Depending on the binary signal values on the control lines 300, 301 and 302 either the gate G or G will be activated for controlling the passage of information to a particular substitution unit S.sub.0 or S.sub.1. Each substitution unit consists of a decoder and encoder section with a random interconnection of wires between the output of the decoder and the input of the encoder, as shown in FIGS. 5A and 5B of application Ser. No. 158,360. By this simple device, it is possible to develop one out of  $2^{sup.n}$  ! possible permutations for n input lines. The substitution as carried out by the S.sub.0 and S.sub.1 units effects a nonlinear transformation of the output of mangler 30.

CLPR:

4. The process as defined in claim 3 wherein pairs of ciphers are generated under alternate control of a subscriber key and a random combination of binary digits.

CLPR:

7. The system as defined in claim 6 wherein said block ciphers generated by said cryptographic device are alternately functions of a combination of binary digits associated with a particular subscriber to a computing network and a random combination of binary digit representations.

CLPV:

a block of binary digits whose combination at any particular time is a random arrangement of one's and zero's.

CLPV:

combining said random combination of binary digits with portions of data segments for generating composite ciphers.